Amendments to the Drawings

As indicated on the attached Replacement Sheet, please amend Fig. 4 to change the word "libre" to "free" as required by the Examiner.

Attachments: One (1) Replacement Sheet

Remarks

The following remarks are responsive to the Office Action of May 21, 2008. At the time of the Office Action, claims 1-30 were pending.

In the Office Action, claims 1-6, 12-15, 16-18, the Abstract, specification and drawings were objected to due to various informalities. In response to these objections, the claims, specification, Abstract and Figure 4 are amended as indicated above in accordance with the Examiner's suggestion.

However, Applicants respectfully traverse the Examiner's objection to reference characters 13, 16 and 17 in Figures 1 and 5, and the Examiner's objection to the use of the term "step 23." Concerning reference character 13, Applicants respectfully submit that using reference character 13 to designate both the transmitting step of y to B and y to C in Figures 1 and 5, respectively, is accurate, since reference 13 clearly refers to transmitting the same element y to a receiver, which is the second entity B in Figure 1 operating as a verifier, and the third entity C that clearly operates as an intermediate entity to the second entity B. Hence, Applicants respectfully submit that is correct to use the same reference character 13 to reference the step of transmitting y regardless of whether y is transmitted to the second entity B or third entity C. For similar reasons, Applicants respectfully submit that it is appropriate to use reference character 16 representing a transition in Figures 1 and 5, and reference character 17 representing a verification operation in Figures 1 and 5.

In the Examiner's objection to Step 23, the Examiner contends that Step 23 is used to designate both generating a first element of proof and a common number. However, Applicants respectfully submit that referring to Figure 2, it is clear that first element of proof x which is obtained from a hash function h( ) and common number c actually refer to the same value, since the common number c is instantiated to the first element of proof x, i.e. c:=x. Consequently, using the same reference "Step 23" is not misleading to one of ordinary skill in the art.

For at least the above reasons, Applicants respectfully request that the Examiner withdraw the formal objections.

Claims 1 and 8 rejected under 35 U.S.C. § 112, second paragraph, as being indefinite. In response, the claims are being amended as indicated above to remove the term "substantially less" from claim 1 and to clarify the term "substantially greater" in claim 8. In view of these amendments, Applicants respectfully request that the Examiner withdraw this rejection.

Turning now to the art-based rejections, Claim 13 was rejected under 35 U.S.C. §102(b) as anticipated by Gilbert et al. (U.S. Patent No. 5,987,138). Claims 1-2, 11, 16 and 17 were rejected under 35 U.S.C. §103(a) as obvious over Gilbert et al. in view of M'Raihi et al. (U.S. Patent No. 5,946,397). Claims 12 and 18 were rejected under 35 U.S.C. §103(a) as obvious over Gilbert et al. in view of M'Raihi et al., and further in view of Brickell (U.S. Patent No. 7,165,181). Claims 19 and 27 were rejected under 35 U.S.C. §103(a) as obvious over Gilbert et al. in view of M'Raihi et al., and further in view of Kasahara et al. (U.S. Patent No. 6,788,788). Claims 3 and 4 were rejected under 35 U.S.C. §103(a) as obvious over Gilbert et al. in view of M'Raihi et al., and further in view of Arditti et al. (U.S. Patent No. 6,125,445). Claims 5-10 and 23-26 were rejected under 35 U.S.C. §103(a) as obvious over Gilbert et al. in view of M'Raihi et al. and Arditti et al., and further in view of Kasahara et al. Claims 20-22 and 28-30 were rejected under 35 U.S.C. §103(a) as obvious over Gilbert et al. in view of M'Raihi et al. and Kasahara et al., and further in view of Arditti. Claim 14 was rejected under 35 U.S.C. §103(a) as obvious over Gilbert et al., and further in view of Kasahara et al. Claim 15 was rejected under 35 U.S.C. §103(a) as obvious over Gilbert et al. in view of Kasahara et al., and further in view of Arditti et al.

Applicants respectfully submit that all claims should be allowable for the reasons discussed below.

The rejection of Claim 13

In this rejection, the Examiner contends that Gilbert anticipates independent claim 13. Applicants respectfully submit that the above amendments to claim 13 render this rejection moot. Applicants submit that the features added by this amendment to claim 13 are similar to those present in dependent claim 2.

Applicants further submit that Gilbert discloses a protocol for identification and/or signature between a claimant (the prover) and a verifier. However, Applicants respectfully submit that in the claimed embodiment of the present invention, the first element of proof x is generated by the prover device by raising the generic number (g) to a second prover modulo, with the modulus (n) having a third exponent equal to the first exponent (e) of the public key multiplied by a random integer (r) kept secret by the first entity or prover device. On the contrary, in the process taught by Gilbert, the element x is obtained by raising a given number (r) to a power modulo the modulus (n) having an exponent equal to the exponent (e) of the public key only.

For at least these reasons, amended claim 13 should be allowable over Gilbert.

The Rejection of Claims 1-2, 11, 16 and 17

In this rejection, the Examiner admits that Gilbert fails to teach the verifying features recited in independent claims 1 and 16. Nevertheless, for these features, the Examiner relies on the teachings of M'Raihi, and contends that one skilled in the art would have found it obvious to have modified Gilbert in accordance with those teachings to have achieved the claimed embodiments of the present invention. Applicants respectfully disagree.

The Examiner contends that Gilbert discloses generating a first element of proof (x) at the first entity (claimant), and generating at the first entity a second element of proof (i.e. the answer y) related to the first element of proof and dependent on a common number (ai). Applicants respectfully submit, however, that although in the embodiments of the invention a

common number c is shared between verifier (A) and prover (B), the second element of proof y as calculated by the first entity A cannot be assessed as being an answer to the verifier B, in the absence of actual transaction from the verifier (B) to the prover (A).

The Examiner further contends that M'Raihi discloses the feature of verifying at the second entity (the verifier) that the first element of proof x is related through a relationship with a first power modulo, with the modulus p of a generic number g having a second exponent k equal to a linear combination of at least part of the common number and of the first exponent of the public key multiplied by the second element of proof. Applicants respectfully submit that although M'Raihi refers to a method based on the discrete logarithm, each entity forms a data base containing a fixed number of exponents and corresponding powers. Hence, Applicants respectfully submit that combining the teachings of Gilbert and M'Raihi, as suggested by the Examiner, will prove inoperative, at least for the following reason.

As taught by Gilbert, element x equals r^e, i.e. $x = r^e$, while element y equals r multiplied by s^a, i.e., $y = rs^a$. Accordingly, Applicants respectfully submit that the Examiner cannot rely on Gilbert's teachings to obtain the claimed equality between the first element of proof x and $g^{(ey+a)}$, i.e., $g^{(ey+a)}$, to have the verifier verifying the first element of proof value x being equal to $g^{(ey+a)}$. Consequently the cryptographic scheme taught by Gilbert, which is based on a Fiat-Shamir or a Guillou-Quisquater approach, and the cryptographic scheme of the claimed invention based on a discrete logarithm approach, are incompatible.

Furthermore, Applicants submit that as clearly stated in column 1, lines 43 to 48 of M'Raihi, the computation of variables $g^k \pmod p$, that is, the computation of variables expressed as modular multiplication operations, is much more costly in terms of computation time and memory space consumption. Applicants submit that Gilbert cannot overcome this drawback, since Gilbert teaches that $y = rs^a \pmod n$. Moreover, M'Raihi does not intend to skip corresponding modular multiplication operations, but operates to lighten the corresponding computation burden.

On the contrary, as would be understood by one skilled in the art, the claimed embodiments of the present invention is able to overcome the above mentioned drawback with regard to the second element of proof y shown as a response, as described, for example, in paragraph [0048] of the corresponding published Patent Application No. US 2005/0213769. Such an advantage is obtained by defining and choosing the elements or variables which are exchanged between the prover and the verifier so as to embody the second element of proof y seen as a response as a simple linear combination.

Accordingly, Applicants submit that for at least the above reasons, one skilled in the art would not have found it obvious to have modified Gilbert in accordance with the teachings of M'Raihi to have achieved the embodiments of the present invention even as recited in independent claims 1 and 16. Hence, all claims should be allowable.

The Rejection of Claims 12 and 18

In this rejection, the Examiner admits that Gilbert and M'Raihi fail to teach the features recited in these claims, but relies on Brickell as allegedly teaching these features. Applicants respectfully disagree.

Claims 12 and 18 are directed to introducing a third (intermediate) entity C to receive the second element of proof y and thus generating and transmitting a third element of proof Y:=gy (mod n) to the second entity B. The Examiner contends that Brickell discloses corresponding features.

However, Applicants respectfully submit that Brickell discloses a challenger (A) requesting that a prover (B) provides information about itself, with the challenger A wanting to establish that the requested information emanates from a device manufacturer (entity) C. The challenger A challenges thus the prover B to show that it possesses the signature generated by entity C.

Applicants thus respectfully submit that Brickell fails to teach the features of the claimed embodiment of the present invention in which the third (intermediate) entity is not a trust entity to second verifier entity B. Instead, in accordance with the claimed embodiments, the third entity C can be entrusted by first prover entity A since it receives its second element of proof y to generate the third element of proof y.

In addition, Applicants respectfully submit that Brickell fails to make up for the deficiencies in the teachings of Gilbert and M'Raihi as discussed above.

Accordingly, for at least these reasons, Applicants respectfully submit that one skilled in the art would not have found it obvious or possible to have combined the teachings of Gilbert, M'Raihi and Brickell to have achieved the embodiments of the present invention even as recited in independent claims 1 and 16. Hence, all claims should be allowable.

The Rejection of Claims 19 and 27

In this rejection, the Examiner admits that Gilbert and M'Raihi fail to teach the features recited in these claims, but relies on Kasahara as allegedly teaching these features. Applicants respectfully disagree.

The Examiner contends that Kasahara discloses that the common number comprises first and second elementary common numbers, the second element of proof is generated by the first entity by subtraction from the random integer multiplied by the first elementary common number, the private key multiplied by the first element common number, the linear combination being equal to the second exponent comprising a zero coefficient for the first elementary common number, a positive unitary coefficient for the first exponent of the public key multiplied by the second element of proof, and, in the verified relationships, the first element of proof is considered with an exponent equal to the first elementary common number. Applicants respectfully submit, however, that although Kasahara is concerned with cryptographic communication between several entities, it actually refers to key sharing functions through ID-NIKS (for ID based Non Interactive Keysharing Scheme) in which an

encryption key is shared, without any precommunication being performed, between a common trusted center and several entities.

Applicants thus respectfully submit that Kasahara fails to teach the features of the embodiments of the present invention as recited in these claims. In addition, Applicants respectfully submit that Kasahara fails to make up for the deficiencies in the teachings of Gilbert and M'Raihi as discussed above.

Accordingly, for at least these reasons, Applicants respectfully submit that one skilled in the art would not have found it obvious or possible to have combined the teachings of Gilbert, M'Raihi and Kasahara to have achieved the embodiments of the present invention even as recited in independent claims 1 and 16. Hence, all claims should be allowable.

The Rejection of Claims 3 and 4

In this rejection, the Examiner admits that Gilbert and M'Raihi fail to teach the features recited in these claims, but relies on Arditti as allegedly teaching these features. Applicants respectfully disagree.

The Examiner contends that Arditti disclose for authentication that a message received by the second entity comes from the first entity, the first element of proof is generated by the first entity by applying a hash function to the message and to the generic number raised to a second power modulo the modulus having a third exponent equal to the first exponent of the public key multiplied by a random integer kept secret by the first entity, with the relationship verified by the second entity being an equality relationship between the first element of proof and a result of the hash function applied to a message and to the first power of the generic number. However, Applicants respectfully submit that as with regard to Gilbert as discussed above, in contradistinction to the claimed embodiments of the present invention, the transaction between the claimant and the verifier takes place thanks to a question T, h sent from the verifier to the claimant.

Accordingly, for at least these reasons, Applicants respectfully submit that one skilled in the art would not have found it obvious or possible to have combined the teachings of Gilbert, M'Raihi and Adritti to have achieved the embodiments of the present invention even as recited in independent claim 1 from which claims 3 and 4 depend. Hence, independent claim 1, and all claims dependent thereon, should be allowable

The Remaining Rejections of the Dependent Claims

In addition to the rejections addressed above, Claims 5-10 and 23-26 were rejected under 35 U.S.C. §103(a) as obvious over Gilbert et al. in view of M'Raihi et al. and Arditti et al., and further in view of Kasahara et al. Claims 20-22 and 28-30 were rejected under 35 U.S.C. §103(a) as obvious over Gilbert et al. in view of M'Raihi et al. and Kasahara et al., and further in view of Arditti. Claim 14 was rejected under 35 U.S.C. §103(a) as obvious over Gilbert et al., and further in view of Kasahara et al. Claim 15 was rejected under 35 U.S.C. §103(a) as obvious over Gilbert et al. in view of Kasahara et al., and further in view of Arditti et al.

Applicants respectfully submit that for reasons similar to those discussed above, one skilled in the art would not have found it obvious or possible to have combined the cited references to have achieved the embodiments of the present invention even as recited in the independent claims. Applicants respectfully note that as discussed above with regard to the rejection of claims 1-2, 11, 16 and 17, the Flat-Shamir or the Guillou-Quisquater approach of Gilbert does not allow one to derive and thus implement a discrete logarithm approach as per the claimed embodiments of the present invention.

Concerning the rejections of claim 14 specifically, the Examiner contends that that Kasahara discloses calculation means which are designed to generate the second element of proof by taking the difference between the random integer and the private key multiplied by the common number, or, the common number being split into two elementary common numbers, by subtracting from the random integer multiplied by the first elementary common number, the private key multiplied by the second elementary common number. However,

Applicants respectfully submit that as discussed above, the teachings of Kasahara relate to only sharing a key.

With regard to the rejection of claim 15 specifically, the Examiner contends that Arditti discloses calculation means being designed to carry out operatives modulo an image of the modulus via a Carmichael function or modulo a multiple of the order of the generic number modulo the modulus. However, Applicants respectfully submit that column 4, lines 48-50 of Arditti do not mention a Carmichael function as recited in claim 15. Furthermore, as discussed above, the teachings of Arditti fail to make up for the teachings of the other references even with regard to claim 13 from which claim 15 depends.

Accordingly, for at least the above reasons, all claims should be allowable.

Conclusion

The application is considered in good and proper form for allowance, and the Examiner is respectfully requested to pass this application to issue. If, in the opinion of the Examiner, a telephone conference would expedite the prosecution of the subject application, the Examiner is invited to call the undersigned attorney.

Respectfully submitted,

/brian c. rupp/

Brian C. Rupp, Reg. No. 35,665
Joseph J. Buczynski, Reg. No. 35,084
DRINKER BIDDLE & REATH LLP
191 N. Wacker Drive, Suite 3700
Chicago, Illinois 60606-1698
(312) 569-1000 (telephone)
(312) 569-3000 (facsimile)
Customer No.: 08968

Date: September 22, 2008
CH01/ 25228262.1